AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with the Facebook user IDs 100021157401739 and 100006311773965 that are stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

Case No. 19-MJ-1291

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. Sections 2251(a) and 2252(a)(4)(B)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christina Porter

Applicant's signature

FBI Special Agent Christina Porter

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 9/10/19

William E. Duffin

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. William E. Duffin, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christina Porter, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored, owned, maintained, controlled, or operated by Facebook, a social network provider located at 1601 Willow Road, Menlo Park, California 94025. The information to be searched consists of two (2) accounts (hereinafter, the Subject Accounts) and is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government copies of the information (including the content of communications) further described in Attachment B.

2. I am a Detective with the West Allis Police Department and am currently assigned to the Sensitive Crimes Unit. I have been a law enforcement officer since May of 2004. As part of my official duties, I am currently assigned as a Task Force Officer (TFO) to the FBI's Child Exploitation Task Force, Milwaukee Division. As part of my duties as a Detective and Task Force Officer, I investigate violations of law relating to child pornography and exploitation. That work frequently includes executing search warrants and conducting interviews of subjects suspected of trading and manufacturing of child pornography or otherwise sexually exploiting children with the use of technology. My duties include investigating criminal violations relating to child exploitation and child pornography including violations of advertising, producing, distributing, receiving, and possessing child pornography, in violation of Title 18, United States Code, Sections 2251 and 2252. I have received training in the investigation of child pornography and child exploitation offenses and have observed and reviewed numerous examples of electronically-stored

child pornography. I have also gained experience in conducting these investigations through my everyday work as a Sensitive Crimes Detective and Task Force Officer.

3. The purpose of this application is to seize evidence more particularly described in Attachment B, of violations of 18 U.S.C. § 2251(a), which makes it a crime to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, and 18 U.S.C. § 2252(a)(4)(B), which makes it a crime to knowingly possesses, or knowingly accesses with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such a visual depiction involves the use of a minor engaging in sexually explicit conduct.

4. The statements contained in this Affidavit are based my experience and background as Sensitive Crimes Detective and Task Force Officer with the FBI, and by information provided by other law enforcement agents. Some information in this affidavit also comes from information received from the issuance of administrative summonses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251 and 2252 is located in the accounts described in Attachment A.

5. More specifically, I seek authorization to search Facebook's information associated with the following individual, whom I have identified by name as well as by Facebook account names:

URL	FACEBOOK ID (UID)	FACEBOOK NAME
https://www.facebook.com/roman.cirino.5	100021157401739	Jose Roman
https://www.facebook.com/josecarlos.roman.758	100006311773965	Jose Carlos Roman

6. The information I seek is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California, from at least approximately January 1, 2015, to the present.

II. DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "Cloud Storage" refers to saving data to an off-site storage system

maintained by a third party. Instead of exclusively storing information to the computer's hard drive or other local storage devices, the user saves it to a remote database (and or both). The Internet provides the connection between the computer and the database. There are several cloud-based storage options available to consumers (Dropbox, Google Drive, Box, Copy, Amazon, One Drive), with the majority of them offering gigabytes of storage free of charge.

d. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

e. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be

stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

f. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

g. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

h. The terms "records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

III. BACKGROUND ON PEOPLE WITH AN INTEREST IN CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

8. Based on my training and experience, as well as the training and experience of other law enforcement personnel with whom I have spoken, I have learned the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, videos, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography, but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer file sharing and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of individuals who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be

maintained in computer storage devices, or in remote storage accounts.

d. Individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. One way to store child pornography without keeping the material on a specific device is to use cloud-based file storage services such as Google Drive, which can be accessed through an internet connection from any computer.

IV. PROBABLE CAUSE

9. On May 4, 2018, Agent Jose Antonio Hernandez-Gomez of the Juncos Municipal Police Department in Puerto Rico provided the Federal Bureau of Investigation (FBI) with information regarding an investigation involving the possession and production of child pornography. The initial complaint was made by the principal where the two juvenile victims attend school. The principal was identified as Diana Inostroza (Diana), who is the principal of Furgencio Pineiro School in Juncos, Puerto Rico.

10. Diana Inostroza reported that a juvenile student at her school is SMA, m/H, 03/07/04 (full name is known by law enforcement). SMA's mother, LAR (full name is known by law enforcement), told Diana that she had located numerous messages and pictures of male genitalia on SMA's cell phone.

11. Agent Hernandez-Gomez interviewed LAR and SMA. SMA said that the person who sent him the naked images on his cell phone was Jose (Jose was later identified by the FBI as Jose Carlos Roman-Cirino, m/H, 01/11/99). In addition, SMA said he sent naked pictures of himself to Jose per Jose's request. SMA told Agent Hernandez-Gomez that he was not the only boy who had received messages and pictures from Jose, and that his friend, ADLJ, m/H, 09/03/04

(full name is known by law enforcement), had also communicated with Jose.

12. Agent Hernandez-Gomez also interviewed ADLJ who said he received messages and photographs from Jose. ADLJ said he received a friend request on Facebook from Jose, which ADLJ accepted. Jose asked ADLJ to introduce him to his male friends. He also asked ADLJ to send him naked pictures of himself, but ADLJ declined.

13. Agent Hernandez-Gomez was provided with the cell phones used by SMA and ADLJ to communicate with Jose. The cell phones were turned over to the FBI, who had the parents of the boys sign Consent to Search forms for the cell phones. FBI Special Agents (SA) Neftali Valdes and Miosotis Ortiz in Puerto Rico then took over the investigation.

14. On May 7, 2018, LAR was interviewed by SA Ortiz at the FBI in Humacao, Puerto Rico. LAR said on April 29, 2018, she did not let her son, SMA, use his cell phone. She put the phone in airplane mode until the next day. Then when she deactivated the airplane mode on April 30, 2018, she observed text messages on the cell phone which included pictures of a male's penis. LAR said some of the messages stated, "llama," meaning call back, and "llama tu," meaning you call back. The contact in the phone who was sending these messages was listed under the name of "Loco." There were also some incoming phone calls from this contact in the phone. LAR said she asked SMA about this person and SMA said he is Jose from his classroom. Then on May 2, 2018, LAR went to SMA's school to report the incident to the principal. The principal then called the Juncos Municipal Police (JMP). A report was taken under case number 2018-6-040-01669.

15. On May 7, 2018, SMA was interviewed by SA Ortiz at the FBI in Humacao, Puerto Rico. SMA said Jose contacted him via text message on his cell phone. SMA said his best friend, ADLJ, had provided Jose with SMA's phone number. Jose told SMA he wanted to know more of SMA's male friends. Jose called SMA several times and Jose said he was 19 years old. SMA said

he saw Jose's face when ADLJ showed SMA Jose's Facebook page. SMA said he talked on the phone with Jose about five times. SMA did not have any social media accounts at the time of the contact.

16. SMA said Jose asked him to send him photographs of his genital area, naked and aroused. SMA sent Jose two photographs on different dates through text messages on his cell phone. SMA said he was naked when he took the photos of himself. SMA said Jose texted him back and said, "que rico," referring to how desirable it was. SMA said one of the photos was taken in his bathroom and one was taken in his bed. SMA said he received three photographs of an aroused penis from Jose, but Jose's face was not in the pictures. Jose requested SMA send him more pictures, and when SMA refused, Jose threatened to show SMA's nude images to other people.

17. SMA also said that Jose asked him and ADLJ to meet in person and that Jose would pick them up. SMA told Jose he did not want to meet and Jose said he would find the boys and rape them. Jose also asked SMA to conduct a video call so Jose could see SMA naked. SMA did not do this and told Jose his phone did not have this capability.

18. On May 7, 2018, SA Ortiz also interviewed ADLJ at the FBI in Humacao, Puerto Rico. ADLJ stated that he received a Facebook friend request from the Facebook profile name of Jose Roman with the URL of https://www.facebook.com/roman.cirino.5. They had one friend in common, so ADLJ accepted the friend request. Jose asked ADLJ for his phone number and ADLJ provided his cell phone number.

19. ADLJ told SA Ortiz that Jose sent ADLJ pictures on his genitals and Jose asked ADLJ to send the same type of pictures back. ADLJ did not send any pictures to Jose. ADLJ said Jose wanted to know who ADLJ's male friends were, so ADLJ provided Jose with SMA's cell

phone number. ADLJ said he spoke on the phone with Jose daily for about one month. They also chatted on Facebook Messenger, WhatsApp, and conducted video calls together. Jose asked to meet with ADLJ in person. ADLJ was unsure if he told Jose his age, but said that he told Jose he was in school and ADLJ said it was obvious from ADLJ's Facebook profile picture that ADLJ is a juvenile because he was wearing his school polo shirt.

20. The phone number used by Jose to communicate with SMA and ADLJ was 262-676-3474. This phone number is also associated with Jose's WhatsApp account per open source records. Accurint and Clear records were checked by FBI agents for these phone numbers, which showed that this phone number belonged to subscriber Jose Carlos Roman-Cirino. Records checks were performed on this name, which showed that Jose was residing at 1902 Hamilton Street in Racine, WI, USA. FBI SOS Hannah Vogel determined through FBI databases that the phone number of 262-676-3474 was assigned to AT&T at the time Jose was contacting the boys. SOS Vogel then issued an administrative subpoena to AT&T and the results came back to the name of Jose Cirino, of 5502 Washington Ave., Mt. Pleasant, WI. The dates of the service through AT&T for this account is 10/19/17 through 10/12/18.

21. The Facebook profile used by Jose to contact ADLJ was "Jose Roman" with a URL of https://www.facebook.com/roman.cirino.5. The Facebook ID number associated with the profile is 100021157401739. On May 22, 2019, I located and reviewed this Facebook profile which was still active. Jose is listed as living in Racine, WI. He is listed as having 4,999 Facebook friends, most of which appear to be young males. The pictures on the profile of Jose match the pictures provided by SA Valdes from Jose's Puerto Rican identification card. On May 22, 2019, I completed a preservation request to Facebook for the account.

22. Agents in San Juan also located a second Facebook account that is believed to be

utilized by Jose with the URL of https://www.facebook.com/josecarlos.roman.758. The images posted on this account appear to be of Jose based on his other Facebook account and his identification card photo. The name on the account is Jose Carlos Roman and the Facebook ID number associated with the profile is 100006311773965. SOS Vogel submitted a preservation request for this account.

23. On March 1, 2019, the Milwaukee Division of the FBI received a lead from SA Valdes requesting agents to conduct surveillance at 1902 Hamilton Street in Racine, WI. Members of the FBI's surveillance team observed Jose at this residence on April 3, 2019. Additional surveillance was conducted on August 20, 2019 and Jose was observed again leaving this residence. He drove to Save-A-Lot Foods where he was then observed working.

24. SA Eliot Mustell of the Milwaukee Division of the FBI advised SA Valdes that we were able to confirm that Jose resided in Racine, WI. SA Mustell requested that the case be further investigated by the Milwaukee Division of the FBI since Jose resided in Wisconsin. On May 21, 2019, SA Mustell requested my assistance with the investigation. SA Mustell and I have been in contact with the Agents in San Juan in regards to obtaining any evidence they have already collected.

25. On July 9, 2019, I received two sets of Blue Ray disks from the FBI in San Juan. These disks contained the Cellebrite reports of the contents of SMA and ADLJ's cell phones. I reviewed the contents of the disks and under the images section of the report for SMA's phone were images of a nude, erect penis. These pictures were sent to SMA's phone from the phone number 262-676-3474, which was entered into SMA's phone as a contact labeled "Loco." They were taken and sent on about 05/02/18. Between May 1, 2018 and May 3, 2018, there were multiple text messages sent by "Loco" to SMA's phone and in many messages, Loco was asking

to call SMA in Spanish. The following is some of the conversation that took place between SMA and Loco:

05/01/18 at 02:40:56 AM from Loco to SMA: "Llama"

05/01/18 at 02:41:00 AM from Loco to SMA: "Que tu ase"

05/01/18 at 02:52:20 AM from Loco to SMA: "Llama"

05/01/18 at 02:52:26 AM from Loco to SMA: "Llama tu"

05/01/18 at 2:52:38 AM from Loco to SMA: "Llama"

One of the messages from May 2, 2018 is as follows:

05/02/18 at 04:50:57 PM from Loco to SMA: "Tequiero"

Some of the messages from May 3, 2018 are as follows:

05/03/18 at 01:53:03 AM from Loco to SMA: "Que tu ase papi"

05/03/18 at 04:59:46 PM from Loco to SMA: "Llama"

05/03/18 at 04:59:50 PM from Loco to SMA: "Llama tu"

I also reviewed the contents of ADLJ's phone and confirmed he had Facebook Messenger and the WhatsApp application on his phone. Within ADLJ's Facebook Messenger chats, I located incoming messages on April 22, 2018 from the Facebook ID number 100021157401739 and name of Jose Roman. There were some attachments sent in these messages from Jose Roman to ADLJ, which included nude images of an erect penis. Jose Roman also wrote, "Tu pene" which translates to "your penis." Jose Roman wrote, "Llama" which translates to "call." ADLJ wrote, "Mi numero es 787 508 1364." The following is a portion of the conversation between Jose Roman and ADLJ on Facebook Messenger:

04/22/18 at 09:18:13 AM Jose Roman to ADLJ: "Hola"

04/22/18 at 10:45:32 AM ADLJ to Jose Roman: "Hola"

04/22/18 at 10:45:43 AM Jose Roman to ADLJ: "Dimelo"

04/22/18 at 10:46:12 AM ADLJ to Jose Roman: "Q hcs"

04/22/18 at 10:47:23 AM Jose Roman to ADLJ: "Yo alado muena caqueta"

04/22/18 at 11:24:41 AM ADLJ to Jose Roman: "Q"

04/22/18 at 11:25:12 AM Jose Roman to ADLJ: image/jpeg

31150349_177521199629…(this was an image of an erect penis under red underwear)

04/22/18 at 11:25:27 AM ADLJ to Jose Roman: three emoji faces

04/22/18 at 11:25:38 AM Jose Roman to ADLJ: "Dale tu"

04/22/18 at 04:57:08 PM ADLJ to Jose Roman: "Es muy poco"

04/22/18 at 04:57:09 PM ADLJ to Jose Roman: "Para mk"

04/22/18 at 04:57:12 PM ADLJ to Jose Roman: "Mi"

04/22/18 at 05:00:07 PM Jose Roman to ADLJ: "Si tu"

04/22/18 at 05:00:14 PM Jose Roman to ADLJ: (this was an image of a nude, erect penis)

04/22/18 at 05:02:05 PM ADLJ to Jose Roman: "Q"

04/22/18 at 05:03:32 PM Jose Roman to ADLJ: "Tu pene"

04/22/18 at 05:05:03 PM ADLJ to Jose Roman: "Pa q maricon"

I also located messages on WhatsApp between ADLJ and an account in the name of "J" with the phone number of 262-676-3474 between the dates of April 22, 2018 and April 26, 2018. Lastly, in the images section of the report there were up-close pictures of a nude, erect penis, but I was unable to determine if the person was an adult or juvenile. There were also pictures of a nude juvenile male posing in a mirror.

26. On July 16, 2019, SA Eliot Mustell utilized an undercover Facebook account to send a friend request to Jose's Facebook account in the name of Jose Roman. Jose accepted the friend request and sent the undercover account messages via Facebook Messenger. Jose also

tried to call the undercover account from the phone number 414-458-5746. SA Mustell asked Jose if he used WhatsApp and Jose said he did. Also on July 16, 2019, SA Mustell located Jose's WhatsApp account, which at this time had the associated phone number of 262-412-5327. On July 16, 2019, SA Mustell and I compared the profile picture on this account to the profile picture for the Jose Roman Facebook profile picture and they appeared to be the same person.

V. FACEBOOK

27. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

28. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

29. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

30. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

31. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

32. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a

user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

33. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

34. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

35. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

36. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

37. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

38. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

39. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

40. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

41. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

42. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

43. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

44. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

45. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and

tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

46. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications).

48. Based on the forgoing, I request that the Court issue the proposed search warrant.

49. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

51. I request that the Court order Facebook not to notify any person (including the subscribers or customers of the account listed in Attachment A) of the existence of the requested warrant before September 1, 2020, or until further order of the Court. Facebook is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, I seek a warrant requiring Facebook to disclose records and information in connection with a criminal investigation. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant … is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant … ." Id.

52. Here, such an order is appropriate because the requested warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the

investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested warrant will seriously jeopardize the investigation, by giving the target an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an investigation. See 18 U.S.C. § 2705(b). Jose Carlos Roman-Cirino is not aware of the investigation into him. If he were to learn the government is investigating him, he could destroy additional evidence of his crimes that may exist and be revealed during the search of his Facebook accounts.

53. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

VII. CONCLUSION

54. Based on ADLJ disclosing that he has had contact with Jose on Facebook since 2018, and that contact includes Jose providing nude images of himself and requesting nude images of ADLJ, and SMA disclosing that Jose exchanged nude images of themselves with one another via text messages, and that ADLJ and SMA both disclosed that Jose asked to be introduced to their other male friends, and that the majority of Jose's Facebook friends are young males, I believe that evidence of the crimes of Title 18, United States Code, Sections 2251 and 2252 will be located in the content of Jose Carlos Roman-Cirino's Facebook accounts between January 1, 2018 and the present time, specifically within the content of Facebook Messenger chats.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user IDs 100021157401739 and 100006311773965 that are stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

ATTACHMENT B

Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(£), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests; including the date and time of the communication, the method of communication, and the source and

destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

(f) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(g) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(h) All "check ins" and other location information;

(i) All IP logs, including all records of the IP addresses that logged into the account;

(j) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(k) All information about the Facebook pages that the account is or was a "fan" of;

(1) All past and present lists of friends created by the account;

(m) All records of Facebook searches performed by the account;

(n) All information about the user's access and use of Facebook Marketplace; and

(o) Records of any Facebook accounts that are linked to the Account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the Account).

(p) The types of service utilized by the user;

(q) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(r) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(s) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

(t) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.